

EXHIBIT G OFF-SITE MODERATE RISK CLOUD COMPUTING SERVICES SECURITY REQUIREMENTS

G1.0 Definitions and Acronyms (Feb 2014)

Definitions and acronyms may be accessed electronically at

<http://www.lanl.gov/resources/assets/docs/Exhibit-G/exhibit-g-definitions-acronyms-green.pdf>

G2.0 Statements Applicable to Scope of Work (Sept 2014)

CONTRACTOR and SUBCONTRACTOR agree and represent that all of the statements listed below are factually correct and applicable to the scope of work (SOW) for this Subcontract. SUBCONTRACTOR has an affirmative duty to immediately notify the Contract Administrator in writing if performance of the SOW contradicts any statement in Section G2.0. In addition, if there is contradiction during the performance of the SOW, CONTRACTOR reserves the right to impose additional security requirements on SUBCONTRACTOR as deemed necessary and appropriate.

- 2.1 Work under this Subcontract will not be performed at any DOE owned or leased facilities including LANL, LANS' leased facilities, or on DOE property.
- 2.2 Access to DOE owned or leased facilities including LANL, LANS' leased facilities, or DOE property will be limited to attending meetings or presentations.
- 2.3 Work under this Subcontract will require approval of a "Cyber Security Plan for Moderate Risk Cloud Services" PRIOR to work beginning.
- 2.4 Work under this Subcontract will require approval of an OPSEC Plan PRIOR to work beginning.
- 2.5 SUBCONTRACTOR workers will not require any LANL security training to perform work under the Subcontract.
- 2.6 SUBCONTRACTOR workers assigned to work on this subcontract and/or have access to data created or provided by CONTRACTOR under this Subcontract ("LANL Data") must be United States Persons, defined as Citizens and Lawful Permanent Residents, except as permitted pursuant to Section G7.0 Foreign Visits and Assignments, herein.
- 2.7 All work under this Subcontract shall be conducted or performed by a company that has been incorporated to do business in the United States.
- 2.8 All LANL Data will be routed and stored on SUBCONTRACTOR systems or servers located solely within the continental United States.
- 2.9 DOE or LANL uncleared or cleared badges will not be required or issued to SUBCONTRACTOR workers performing work under this Subcontract.
- 2.10 Access to OUO, LPI and UCNI information or data will be granted on a need-to-know basis only and shall be protected in accordance with US Government policy.
- 2.11 SUBCONTRACTOR workers will not have access to or process any LANL classified information or matter.
- 2.12 SUBCONTRACTOR workers will not have access to LANL networks or systems requiring authentication; excluding the LANL Visitor network, when applicable.
- 2.13 All LANL Data created or provided under this Subcontract is and shall remain the property of CONTRACTOR or the United States Government and shall in no way become attached to the services under this Subcontract, nor shall SUBCONTRACTOR have any rights to the data.

G3.0 Security Requirements (Sept 2014)

SUBCONTRACTOR shall ensure compliance with all security requirements specified in this Subcontract and all documents incorporated by reference. All measures taken by CONTRACTOR to correct SUBCONTRACTOR Workers' non-compliance shall be at SUBCONTRACTOR'S expense and the cost thereof, including any stipulated penalties resulting from such non-compliance, shall be deducted from payments otherwise due SUBCONTRACTOR.

3.1 DEAR Clauses Incorporated By Reference

- 3.1.1 The Department of Energy Acquisition Regulation (DEAR) clauses and Federal Acquisition Regulation (FAR) clauses that are incorporated by reference herein shall have the same force and effect as if printed in full text.
- 3.1.2 Full text of the referenced clauses may be accessed electronically at <http://farsite.hill.af.mil/VFDOE1.HTM>
- 3.1.3 The following alterations apply only to FAR and DEAR clauses and do not apply to DOE or NNSA Directives. Wherever necessary to make the context of the unmodified DEAR clauses applicable to this Subcontract:
- The term "Contractor" shall mean "SUBCONTRACTOR;"
 - The term "Contract" shall mean this Subcontract; and
 - The term "DOE", "Government," "Contracting Officer" and equivalent phrases shall mean CONTRACTOR and/or CONTRACTOR'S representative, except the terms "Government" and "Contracting Officer" do not change when a right, act, authorization or obligation can be granted or performed only by the Government or the prime contract Contracting Officer or his duly authorized representative; or where specifically modified herein.
- 3.1.4 The following clauses apply as stated in the Instructions:

Clause Number	Title and Date	Instructions
DEAR 952.204-77	Computer Security (Aug 2006)	Applies when Subcontractor has access to computers owned, leased or operated on behalf of the DOE.
FAR 52.204-9	Personal Identity Verification of Contractor Personnel (Jan 2011)	Applies when Subcontractor has routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system.

3.2 DOE Directives Incorporated By Reference

SUBCONTRACTOR shall provide such information, assistance and support as necessary to ensure CONTRACTOR'S compliance with the following DOE/NNSA Directives, as applicable. In addition, SUBCONTRACTOR shall comply with the requirements of the Contractor Requirement Document (CRD) attached to a Directive when required by such CRD. The Directives are prefaced with certain conditions for applicability to the Subcontract. A referenced Directive does not become effective or operative under this Subcontract unless and until the conditions precedent are met through the scope of work. The DOE Directives referenced herein may be found at <http://www.directives.doe.gov/>

Directive Number	Title	Instructions
DOE O 142.3A	Unclassified Foreign Visits and Assignment	Applies if contract involves foreign national access to DOE-owned or leased sites/facilities. Applies if contract involves off-site foreign national access to DOE information or technologies that are not releasable to the public.
NAP 14.1C Chpt. VII	NNSA Baseline Cyber Security Program, Chapter VII Incident Management	Applies if contract work involves information systems used on behalf of DOE/NNSA to collect, process, store, display, create, disseminate or transmit national security or unclassified DOE / government information.
NAP 14.1D	Baseline Cyber Security	Applies if contract involves National Security Systems that collect, process, store, display, create, disseminate, or transmit information.
DOE O 205.1B Chg 1	Department of Energy Cyber Security Program	Applies if contract includes access to DOE unclassified or classified information and information systems used or operated by CONTRACTOR.

Directive Number	Title	Instructions
DOE O 471.6 Chg 1	Information Security	Applies if contract includes access to unclassified or classified information and matter controlled by statutes, regulation or NNSA policies.
DOE O 471.1B	Identification and Protection of Unclassified Controlled Nuclear Information	Applies to work activities that may generate, possess, or have access to information or matter containing UCNI.
DOE O 471.3	Identifying Official Use Only Information	Applies if contract involves activities where Official Use Only (OUO) information and documents will be handled, used or generated.
DOE M 471.3-1	Manual for Identifying and Protecting Official Use Only Information	Applies if contract involves activities where Official Use Only (OUO) information and documents will be handled, used or generated.
DOE O 475.1	Counterintelligence Program	Applies if contract work involves access to or use of DOE facilities, technology, personnel, unclassified sensitive information and classified matter.

G4.0 Operations Security (Sept 2014)

SUBCONTRACTOR shall develop, with assistance from CONTRACTOR's Physical Security group, implement and sustain a DOE OPSEC Plan using the template provided by the Contract Administrator / Procurement Specialist. SUBCONTRACTOR'S OPSEC Plan shall be approved by CONTRACTOR'S Physical Security group before work may begin for LANL. A link to the OPSEC Plan Template is <http://www.lanl.gov/resources/exhibit-g.php>

G5.0 Reporting Security Incidents (Sept 2014)

This subsection contains requirements for reporting potential and known incidents of security concern. Such incidents may involve issues associated with Personally Identifiable Information (PII), computer systems, secure communications, personnel security, and physical security occurring on LANL property, Laboratory-leased property or SUBCONTRACTOR-owned property. Subcontract workers shall comply with the following requirements.

- 5.1 Immediately upon discovery of a potential incident of security concern, report such concern to the Security Incident Team (SIT) (505-665-3505) or a SPL / DSO; and inform the RLM, and STR/AdSTR. During normal business hours, notifications shall be made only in person or through secure communications (STU or STE) as required below. A non-secure telephone, non-secure fax, non-secure voice mail, or non-secure electronic mail shall not be used to report a potential incident of security concern.
 - 5.1.1 The potential compromise of PII shall be reported *immediately* upon discovery to the SIT (505-665-3505) or the LANL SPL / DSO. A potential compromise of PII is considered a serious information security incident because of the possibility of significant adverse consequences to the individual whose data has been compromised.
 - 5.1.2 *Immediately* report all security incidents and potential threats and vulnerabilities involving DOE/NNSA and LANL data utilized by the SUBCONTRACTOR to the SIT or the LANL SPL / DSO; and then notify the appropriate ISSO or OCSR, RLM and STR/AdSTR.
- 5.2 Contact Requirements Outside of Normal Business Hours

For all incidents contact the ADSS duty officer through the Protective Force at 505-665-7708, *immediately* after discovery of a potential incident of security concern. The ADSS on-call duty officer (505-949-0156) may ask to meet with the SUBCONTRACTOR in person so that SUBCONTRACTOR may report such known or potential incidents of security concern, if secure communications are not available.

G6.0 Cloud Computing Services (Sept 2014)

SUBCONTRACTOR shall comply with cloud computing services requirements outlined in the following subsections for the use of cloud services. A cloud service denotes any connection that involves delivering host services over the Internet.

6.1 Qualification and Validation

SUBCONTRACTORS shall comply with the following regulations and requirements:

- National Institute of Science Technology (NIST 800-53) found at <http://csrc.nist.gov/publications/PubsSPs.html> or equivalent approved by the CSSM
- Federal Information Processing Standard (FIPS) Publication 199 found at <http://csrc.nist.gov/publications/PubsFIPS.html>

Compliance with these requirements shall be verified by LANL Cyber Information Security prior to SUBCONTRACTOR submitting a formal response to a Request for Proposal. Only those SUBCONTRACTORS who meet the minimum qualifications shall be authorized to provide service.

6.2 Certification and Accreditation

SUBCONTRACTOR shall develop, with the assistance of the LANL Information Cyber Security Office, the following plans prior to the use of a cloud service. These plans must be approved by LANL Cyber Information Security before an Approval to Operate notice is issued.

If SUBCONTRACTOR is already federally authorized or industry tested and authorized, additional certification or accreditation is not required. The following supporting documentation will still be required.

- Security Assessment Report
- System Security Plan or equivalent
- Configuration Management Plan
- Contingency Plan with Business Impact Analysis
- Continuous Monitoring Plan
- Privacy Impact Assessment (PIA) (if LANL PII is going to be stored)
- Interconnection Agreement; Service Level Agreement; Memorandum of Agreement

Additional documentation may be required and requested by the LANL Information Cyber Security Office.

SUBCONTRACTOR shall provide results of annual security control test results to the LANL Information Cyber Security Office. The annual control test shall include:

- Copies of annual assessment reports
- Copies of Business Impact Analysis and IT Contingency Plan annual test reports
- Copies of annual vulnerability assessments

A list of the control tests required can be found at <http://www.lanl.gov/resources/assets/docs/Exhibit-G/nist-800-53.pdf>

G7.0 Foreign Visits & Assignments (Feb 2014)

Approval for a foreign national (not a United States Person, defined as a Citizen or Lawful Permanent Resident) to work on a LANL project or access LANL data off-site must be obtained from the LANL Foreign Visits and Assignments office PRIOR to commencing work on the Subcontract.

G8.0 Substance Abuse (Feb 2014)

8.1 CONTRACTOR Policy

The unauthorized use of alcohol and/or illegal drugs or being under the influence of alcohol and/or illegal drugs by SUBCONTRACTOR workers is prohibited by this Subcontract. LANL's substance abuse policy applies to all who perform work for LANL. SUBCONTRACTOR workers shall be fit for duty and avoid behavior that compromises the security of DOE & NNSA security interests and government protected data. The use of medical marijuana is illegal under federal law and therefore is prohibited in accordance with these substance abuse requirements.

8.2 Off-site Behavior

The unlawful manufacture, distribution, dispensing, possession, use, transfer or sale of controlled substances by SUBCONTRACTOR workers is prohibited by this Subcontract regardless of whether these activities occur at the workplace, on Laboratory business, or on an individual's private time or property. These and other violations of LANL's substance abuse policy are considered connected to work with or at LANL and may result in the termination of a SUBCONTRACTOR worker's permission to work on this Subcontract, regardless of whether or not the misconduct occurs during work hours or off Laboratory premises.

G9.0 Information Security (Feb 2014)

9.1 Official Use Only (OUO) and LANS Proprietary Information (LPI)

OUO and LPI information is unclassified with the potential to damage government, commercial or private interests if disseminated to persons who do not have a need-to-know the information to perform their jobs or other DOE-authorized activities. SUBCONTRACTOR shall protect such information from unauthorized dissemination and shall follow all requirements for OUO and LPI documents specified below.

9.1.1 Access

No security clearance is required for access to OUO or LPI.

If OUO information is Export Control Information (ECI) access is restricted to US persons, defined as citizens and Lawful Permanent Residents.

If OUO information is Applied Technology (AT) it is subject to access restrictions established by the DOE Program Office. The associated LANL program manager can determine access authorizations for Laboratory workers.

9.1.2 Storing

OUO and LPI information shall be stored in a locked room or locked receptacle (e.g. desk, file cabinet, safe). OUO and LPI information stored on a computer shall have passwords, authentication, encryption or file access controls in place for protection.

9.1.3 Transmitting

E-mail messages that contain OUO or LPI information should indicate OUO or LPI in the first line, before the body of the text. OUO or LPI disseminated over networks outside of LANL should be encrypted with NIST-validated encryption software (e.g., Entrust®).

In the case of hard copies being sent outside of LANL, OUO or LPI shall be placed in a sealed, opaque envelope marked with the recipient's name, a return address and the words "To Be Opened by Addressee Only". For interoffice mail within LANL, OUO or LPI shall be placed in a sealed, opaque envelope with the recipient's address and the words "To be Opened by Addressee Only" on the front of the envelope.

9.1.4 Destroying

Users are not required to destroy electronic media that contains OUO or LPI. However, disks should be overwritten using approved software before they are thrown away. Hard copy OUO or LPI documentation shall be destroyed by using an approved shredder.

9.2 Unclassified Controlled Nuclear Information (UCNI)

UCNI is certain unclassified but sensitive government information whereby unauthorized dissemination is prohibited. UCNI is intended to be viewed only by those individuals with a need-to-know the specific UCNI to perform their official duties or DOE-authorized activities. SUBCONTRACTOR shall protect such information from unauthorized dissemination and shall follow all requirements for UCNI documents specified below.

9.2.1 Access

No security clearance is required for access to UCNI; however, access is permitted only to those authorized for routine or special access and those who have a need-to-know. UCNI stored on a computer shall be restricted (passwords, authentication, file access control encryption and offline storage) to only those who have a need-to-know.

9.2.2 Storing

When using UCNI, physical control shall be maintained over the material to prevent unauthorized access to the information. When not in use, UCNI matter shall be stored in a locked room or receptacle (e.g. desk, file cabinet, bookcase or safe). The locked receptacle shall have controls that limit access to only approved workers. UCNI stored on a computer shall have passwords, authentication, encryption or file access controls in place for protection.

9.2.3 Transmitting

Ensure that UCNI is marked correctly prior to transmitting it over any media. Only a qualified Reviewing Official can identify and mark UCNI. Contact the Classification Group through the RLM or STR/AdSTR for assistance.

When transmitting over telecommunication circuits (including telephone, fax, radio, e-mail or Internet) encryption algorithms that comply with all applicable Federal laws, regulations and standards for the protection of UCNI shall be used.

Transmission over open phone lines is prohibited. A Secure Terminal Equipment (STE) line is required. All cellular devices, including LANL-issued smart phones such as Blackberries must be turned off completely when in proximity to UCNI discussions.

UCNI documents must be transmitted using a fax machine that employs encryption. When transmitted outside LANL, UCNI shall be encrypted with NIST-validated encryption software. E-mails with UCNI attachments are considered transmittal documents and shall be marked as such.

When mailing outside of LANL, an opaque envelope shall be used and the outer packaging shall not indicate that the content within is UCNI. For interoffice mail, an interoffice envelope shall be used and mailed through standard interoffice mail, but do not indicate that the content is UCNI. When using e-mail, UCNI shall be encrypted with NIST-validated encryption software such as Entrust®.

9.2.4 Destroying

Users are not required to destroy electronic media that contain UCNI. Disks should be overwritten using approved software before they are discarded. Hard copy UCNI documents are to be destroyed by shredding in an approved shredder. SUBCONTRACTOR shall coordinate with the Classified Matter Protection and Control Team through the RLM or STR/AdSTR to properly destroy UCNI information.

9.2.5 Noncompliance Consequences

SUBCONTRACTOR'S failure to comply with the requirements pertaining to UCNI may result in the imposition of a civil and/or criminal penalty for each violation.

G10.0 U.S. Export Control Requirements (Feb 2014)

SUBCONTRACTOR shall comply with all U.S. export control laws and regulations, including the provisions of the Export Administration Act of 1979 and the U.S. Export Administration Regulations (15 C.F.R. 730-774) promulgated thereunder, the U.S. Department of Energy's export regulations (10 C.F.R. Part 810), the Arms Export Control Act, the International Traffic in Arms Regulations, and the sanctions and laws administered by the U.S. Treasury Department, Office of Foreign Assets Control (OFAC).

SUBCONTRACTOR acknowledges that these statutes and regulations impose restrictions on the import and export to foreign countries and foreign nationals of certain categories of items and data and that licenses from the U.S. Department of Energy, U.S. Department of Commerce, U.S. State Department and/or OFAC may be required before such items or data can be disclosed, and that such licenses may impose further restrictions on use of and further disclosure of such data.

SUBCONTRACTOR further acknowledges that the information which CONTRACTOR may disclose to SUBCONTRACTOR pursuant to the Subcontract may be subject to these statutes and regulations.

G11.0 CONTRACTOR Reviews and Approvals

The undersigned CONTRACTOR representative has reviewed the SOW for the proposed Purchase Request referenced in the footer of this document and represents that all statements listed in Section G2.0 are factually correct.

_____ Name of DSO or SPL	_____ Signature	_____ Date
_____ Name Cyber Security Designee	_____ Signature	_____ Date